I CLAIM AS MY INVENTION:

1. A method for variably generating cryptographic securities, for communications, in a host device, comprising the steps of:

for cryptographically securing a communication for a first purpose, using a first signature;

for cryptographically securing a communication for a second purpose, using a second signature; and

using a cryptographic algorithm of a first type to generate said first signature and using a cryptographic algorithm of a second type to generate said second signature.

2. A method as claimed in claim 1 comprising:

storing a program in a read only memory of a postal security device for implementing the respective cryptographic algorithms for generating said first and second signatures; and

implementing at least one of the cryptographic algorithms for generating at least one of the first and second signatures in a hardware unit outside of and in communication with said postal security device.

3. A method as claimed in claim 1 comprising implementing the respective cryptographic algorithms to generate said first and second signatures in respective, separate logic modules, and generating the first and second signatures in the respective logic modules under control of a program.

4. A method as claimed in claim 1 comprising:

storing a plurality of signing algorithms and hash algorithms in a read only memory of a postal security device; and in a logic module having access to said read only memory, implementing at least one of said signing algorithms and hash algorithms as a cryptographic algorithm for generating one of said first and second signatures, dependent on whether the communication is for said first purpose or said second purpose.

5. A method as claimed in claim 4 comprising implementing said at least one of said signing algorithms and hash algorithms exclusively in said logic module alone.

6. A method as claimed in claim 4 comprising storing an implementation program in said postal security device and implementing said at least one of said signing algorithms and hash algorithms in said logic module using said implementation program.

7. A method as claimed in claim 4 comprising storing an implementation program in said host device and implementing said at least one of said signing algorithms and hash algorithms in said logic module using said implementation program.

8. An arrangement for variably generating cryptographic securities, for communications, in a host device, comprising:

a postal security device having an information input;

a cryptologic module external to said postal security device, having an output connected to said information input of said postal security device, said cryptologic module supplying a cryptoalgorithm at said output; and

a logic circuit in said postal security device, connected to said information input, which applies a digital signal algorithm to said cryptoalgorithm output from said cryptologic module, to generate data for a signature.

9. An arrangement as claimed in claim 8 wherein said cryptologic module has a control data input for receiving control data generated by said host device to modify said cryptoalgorithm output.

10. An arrangement as claimed in claim 9 wherein said cryptologic module comprises a plurality of logic circuits that affect said cryptographic output and a switch connected between each of said logic circuits and said cryptoalgorithm output, and connected to said control data input for connecting one of said logic circuits to said cryptoalgorithm output dependent on said control data.

11. An arrangement as claimed in claim 10 wherein a first of said logic circuits contains a first cryptoalgorithm and a second of said logic circuits contains a second cryptoalgorithm, and wherein said switch connects one of said first cryptoalgorithm and said second cryptoalgorithm to said cryptoalgorithm output dependent on said control data.

12. An arrangement as claimed in claim 8 wherein said postal security device comprises a first logic circuit containing a first cryptoalgorithm, in addition to said logic circuit that generates said data for a signature, and wherein said cryptologic module comprises a second logic circuit containing a second cryptoalgorithm and a third logic circuit containing a third cryptoalgorithm, each of said first, second and third logic circuits having an input and an output, the output of said first logic circuit being connected to said information input of said postal security device and the respective outputs of said second and third logic circuits being connected to said cryptoalgorithm output of said cryptologic module, and said cryptologic module further comprising a switch having outputs respectively connected to the inputs of said first, second and third logic circuits and an input supplied with a communication from said host device, and having a control data input

supplied with control data from said host device to supply said communication to one of said first, second or third logic circuits dependent on said control data.

13. An arrangement as claimed in claim 8 wherein said cryptologic module comprises a first logic circuit containing a first cryptoalgorithm, having an input to which a communication is supplied by said host device, and having an output, and a second logic circuit a second cryptoalgorithm having an input connected to said output of said first logic circuit and an output forming said cryptoalgorithm output of said cryptologic module.

14. An arrangement as claimed in claim 13 wherein said second logic circuit has a key input, and wherein said cryptologic module comprises a switch having a plurality of inputs to which respective cryptographic keys are supplied, and an output connected to said key input of said second logic circuit and a control data input to which control data are supplied by said host device for supplying said key input with one of said cryptographic keys, dependent on said control data, for use in said second cryptoalgorithm.

15. An arrangement as claimed in claim 14 wherein said switch is a first switch and wherein said control data are first control data, and wherein said cryptologic module comprises a second switch having inputs respectively connected to the output of said first logic circuit and the output of said second logic circuit, and an output forming said cryptoalgorithm output of said cryptologic module, and having a control data input supplied with said second control data from said host device, said second switch, dependent on said second control data, connecting the output of one of said first logic circuit or said second logic circuit to said cryptoalgorithm output.

16. An arrangement as claimed in claim 8 wherein said postal security device comprises a first logic circuit, in addition to said logic circuit that generates said data for said signature, containing a first cryptoalgorithm, said first logic circuit having an input supplied with a communication from said host device, and an output, and wherein said cryptologic module comprises a second logic circuit containing a second cryptoalgorithm, said second logic circuit having an input connected to the output of said first logic circuit, a key input, and an output forming said cryptoalgorithm output of said cryptologic module, and said cryptologic module comprising a first switch having inputs respectively supplied with different cryptographic keys, an output connected to said key input, and a control data input supplied with first control data from said host device for supplying one of said different keys to said second logic circuit for use in said second cryptoalgorithm, and wherein said postal security device comprises a second switch having inputs respectively connected to the output of said first logic circuit and to said cryptoalgorithm output of said cryptologic module, an output connected to said logic circuit that generates said signature, and a control data input supplied with second control data by said host device for connecting the output of one of said first logic circuit or said second logic circuit to said logic circuit that generates said signature.

17. An arrangement as claimed in claim 8 wherein said postal security device comprises a first logic circuit containing a first cryptoalgorithm, in addition to said logic circuit that generates said data for a signature, and wherein said cryptologic module comprises a second logic circuit containing a second cryptoalgorithm and a third logic circuit containing a third cryptoalgorithm, each of said first, second and third logic circuits having an input and an output, the output of said first logic circuit being connected to said information input of said postal security

device and the respective outputs of said second and third logic circuits being connected to said cryptoalgorithm output of said cryptologic module, and said postal security device further comprising a switch having outputs respectively connected to the inputs of said first, second and third logic circuits and an input supplied with a communication from said host device, and having a control data input supplied with control data from said host device to supply said communication to one of said first, second or third logic circuits dependent on said control data.

18. An arrangement as claimed in claim 8 wherein said cryptologic module comprises a first logic circuit containing a first cryptoalgorithm and having an input supplied with a communication from said host device, and an output, and a second logic circuit containing a second cryptoalgorithm having an input connected to the output of said first logic circuit and an output forming said cryptoalgorithm output of said cryptologic module, and wherein said postal security device comprises a third logic circuit, in addition to said logic circuit that generates said signature, containing a third cryptoalgorithm and having an input connected to the output of said first logic circuit, and wherein said postal security device contains a switch having inputs respectively connected to the outputs of said first logic circuit, said second logic circuit and said third logic circuit, an output connected to said logic circuit that generates said signature, and a control data input supplied with control data by said host device for connecting one of the outputs of the first logic circuit, the second logic circuit or the third logic circuit to said logic circuit that generates said signature.

19. An arrangement as claimed in claim 8 wherein said cryptologic module comprises a first logic circuit containing a first cryptoalgorithm and having an input supplied with a communication from said host device, and an output, and a second logic circuit containing a second cryptoalgorithm having an input connected to the

output of said first logic circuit, and a third logic circuit containing a third cryptoalgorithm and having an input connected to the output of said second logic circuit and an output forming said cryptoalgorithm output of said cryptologic module, and wherein said postal security device contains a switch having inputs respectively connected to the outputs of said first logic circuit, said second logic circuit and said third logic circuit, an output connected to said logic circuit that generates said signature, and a control data input supplied with control data by said host device for connecting one of the outputs of the first logic circuit, the second logic circuit or the third logic circuit to said logic circuit that generates said signature.